CLAIMS

What is claimed is:

1. An electronic device network for updating at least one of firmware and software in a plurality of electronic devices using at least one electronic device update, at least one of the firmware and software in the plurality of electronic devices and the at least one update being encrypted, the network comprising:

at least one update generator adapted to generate updates, the at least one update generator comprising an encrypting and decrypting engine;

at least one update store storing a plurality of electronic device updates; and

at least one update delivery server adapted to dispense the plurality of electronic device updates.

2. The network according to claim 1, wherein the at least one update delivery server comprises secure sockets layer support providing authentication and data encryption/decryption.

3. The network according to claim 1, wherein each of the plurality of electronic devices are adapted to retrieve secure encrypted updates from the at least one update delivery server to update the at least one of firmware and software resident in the plurality of electronic devices, and wherein at least a portion of the at least one of firmware and software resident in the electronic devices is encrypted.

4. The network according to claim 1, wherein each of the plurality of electronic devices comprise:

one of encrypting and decrypting components; and

a client for downloading updates.

5. The network according to claim 1, wherein each of the plurality of electronic devices comprise a security services component providing secure communication with the at least one update delivery server.

6. The network according to claim 1, wherein each of the plurality of electronic devices comprise an encrypted section, the encrypted section comprising at least one of an encrypted data section and an encrypted code section.

7. The network according to claim 1, wherein each of the plurality of electronic devices comprises at least one of a random access memory, a provisioned data section, an operating system, an update agent, and an update application loader, and wherein the provisioned data section comprises an update agent provisioning information section and a number assignment module.

8. The network according to claim 7, wherein the update agent is adapted to employ at least one of encrypting and decrypting components to update at least one of firmware and software resident in the electronic devices, and wherein at least a portion of the at least one of firmware and software is encrypted and stored in one of an encrypted data section and an encrypted code section.

9. The network according to claim 1, wherein the update generator is adapted to process an old memory image and a new memory image of the at least one of firmware and software in the electronic devices, and wherein at least a portion of the at least one of firmware and software is encrypted.

10. The network according to claim 1, wherein the update generator is adapted to decipher one of encrypted data segments and encrypted code in both an old memory image and a new memory image to generate an update for updating at least one of firmware and software in the electronic devices.

11. The network according to claim 1, wherein the update generator is adapted to employ deciphering techniques to extract one of enciphered code and enciphered data segments, process the one of enciphered code and enciphered data segments to generate an update comprising difference information, and encipher the one of code and data segments, and the difference information in at least one update.

12. The network according to claim 1, wherein the electronic devices comprise a plurality of mobile electronic devices, and wherein the plurality of mobile electronic devices comprise at least one of a mobile cellular phone handset, personal digital assistant, pager, a multimedia player, and a camera.

13. A method of encrypting update information within a firmware image in electronic devices, the method comprising:

creating encrypted updates for an electronic device using binary differencing information; and

encrypting firmware images by applying at least one of stream symmetric enciphering and block symmetric enciphering.

14. The method according to claim 13, wherein stream symmetric enciphering is performed in a byte by byte manner, wherein update information is processed using a key stream to produce an encrypted update.

15. The method according to claim 14, wherein stream symmetric enciphering further comprises an i^{th} byte of the key stream operating on a byte of the update information produce an i^{th} cipher encrypted byte.

16. The method according to claim 15, wherein the i^{th} cipher encrypted byte is decrypted by the i^{th} byte of the key stream operating on the i^{th} cipher encrypted byte to reproduce an original i^{th} byte of update information.

17. The method according to claim 13, wherein block symmetric enciphering is performed upon blocks of data, wherein the blocks of data comprise a predetermined number of bytes, wherein a key block is applied to an update information block to produce an encrypted block, and wherein block symmetric enciphering is performed by cipher block chaining.

18. The method according to claim 17, wherein the predetermined number of bytes in the blocks of data comprises 8-16 bytes.

19. The method according to claim 17, wherein block symmetric enciphering is enabled to accommodate variable block sizes, wherein block sizes are at least one of expanded and padded, wherein padding is one of added and removed to vary the block sizes during a ciphering process.

20. The method according to claim 13, wherein an enciphering algorithm and an enciphering key are stored in the electronic devices.

21. The method according to claim 13, wherein the electronic devices comprise a plurality of mobile electronic devices, and wherein the plurality of mobile electronic devices comprise at least one of a mobile cellular phone handset, personal digital assistant, pager, multimedia player, and a camera.

22. An electronic device employing one of encrypting and decrypting techniques to update firmware and software, the electronic device comprising:

random access memory; and

non-volatile memory, the non-volatile memory comprising:

an update agent;

a first in first out (FIFO) memory device;

a firmware;

a software application; and

an update, wherein the electronic device is adapted to be updated by performing the update upon at least one of the firmware and the software application selected for updating.

23. The electronic device according to claim 22, wherein the at least one of the firmware and the software application selected for updating in the electronic device are at least partially encrypted.

24. The electronic device according to claim 22, wherein the electronic device is adapted to retrieve secure encrypted updates from an update delivery server to update at least one of the firmware and the software application selected for updating resident in the electronic device.

25. The electronic device according to claim 22, wherein the electronic device comprises at least one of encrypting and decrypting components and a client for facilitating downloading updates.

26. The electronic device according to claim 22, wherein the electronic device comprises a security services component providing secure communication with an update delivery server.

27. The electronic device according to claim 22, wherein the electronic device comprises an encrypted section, the encrypted section comprising at least one of an encrypted data section and an encrypted code section.

28. The electronic device according to claim 22, wherein the electronic device further comprises at least one of a provisioned data section, an operating system, an update agent, and an update application loader, the provisioned data section comprising an update agent provisioning information section and a number assignment module.

29. The electronic device according to claim 28, wherein the update agent is adapted to employ at least one of encrypting and decrypting components to update at least one of firmware and software application resident in the electronic device, and wherein at least a portion of the at least one of firmware and software application is encrypted and stored in one of an encrypted data section and an encrypted code section.

30. The electronic device according to claim 21, wherein the electronic device comprises a plurality of mobile electronic devices, and wherein the plurality of mobile electronic devices comprise at least one of a mobile cellular phone handset, personal digital assistant, pager, multimedia player, and a camera.

31. A method of building a firmware upgrade for use in an electronic device incorporating encryption, the method comprising:

building a firmware image to be encrypted, the firmware image comprising a plurality of components; and

encrypting the components before assembling the components into an encrypted firmware image.

32. The method according to claim 31, further comprising:

generating binary difference information between firmware versions undergoing an upgrade; and

using an un-encrypted firmware image to generate the binary difference information, wherein as the upgrade is being applied to an encrypted firmware image, uncorrelated information is decrypted.

33. The method according to claim 31, further comprising creating a data update package, the data update package being based upon un-encrypted binary images.

34. The method according to claim 31, further comprising creating a data update package, the data update package being based upon encrypted binary images.

35. The method according to claim 31, further comprising at least one of:

managing encrypted information by performing a pre-check analysis;

managing encrypted information by performing a check-recovery analysis; and

managing encrypted information by performing a fault tolerant procedure.

36. The method according to claim 35, wherein during at least one of the pre-check analysis and the check recovery analysis, a cyclic redundancy check of a firmware image block is compared against an original image cyclic redundancy check stored in a data update package, wherein when ciphered data is present, the pre-check analysis is performed upon the block to be decrypted before the cyclic redundancy check is calculated.

37. The method according to claim 36, wherein cyclic redundancy check values for ciphered data are stored in the data update package.

38. The method according to claim 35, wherein during the fault tolerant procedure a ciphering algorithm is applied to facilitate recovery of data for the upgrade.

39. The method according to claim 31, further comprising:

decrypting an original data block and copying the decrypted data block to random access memory;

applying update information to the random access memory, the update information comprising at least one of an update code and an update data segment from a data update package;

updating the decrypted data block with the update information to form an updated decrypted data block;

encrypting the updated decrypted data block to form an encrypted updated data block;

sending the encrypted updated data block to a storage unit;

overwriting the original data block with the encrypted updated data block; and

processing every data block to be updated during an upgrade.

40. The method according to claim 39, further comprising a fault tolerant upgrade, the fault tolerant upgrade at least comprising:

maintaining each original data block intact until the original data block is overwritten by an encrypted updated data block; and

maintaining a data update package intact throughout the fault tolerant upgrade.

41. The method according to claim 31, wherein the electronic device comprises a plurality of mobile electronic devices, and wherein the plurality of mobile electronic devices comprise at least one of a mobile cellular phone handset, personal digital assistant, pager, multimedia player, and a camera.